Low Error Detection in Image Watermarking Using DCT

Li Chen[1, a]

[1] Department of Electronic and Information Engineering, Shantou University,
Shantou 515063, Guangdong, P. R. China

[a] lchen@stu.edu.cn

Keywords: Watermark detection; DCT; DHT; integer-valued;

Abstract. Due to round-off errors, watermark detection may not be perfect in the absence of attacks. In this paper, watermarks are adjusted so that the watermarked image is integer-valued. Near-perfect detection is achieved by the DC components of DCT and approximation images. Perfect detection is achieved by full-band watermarking. Although the adjusted watermark is image-dependant, it need not be stored in a watermark bank, as it can be generated from an original watermark and a host image. In this paper, the DC components of discrete cosine transform (DCT) and discrete Hadamard transform (DHT) are shown to be able to attain near-perfect detection, while perfect detection is achieved by full-band watermarking. Time-domain watermarking is not band-limited and hence is equivalent to full-band watermarking.

Introduction

In recent years, digital watermarking technology is becoming increasingly important for on-line services and electronic commerce in wired and wireless connections to the Internet. Invisible digital watermarking techniques embed information inside multimedia data with unperceivable changes of the original data. Steganography techniques also embed information inside multimedia data. These two classes of techniques are similar in a number of respects. One of differences between watermarking and steganography resides in the fact that watermarking requires stronger robustness. Non-fragile watermarking embeds a watermark that is difficult to be removed, even though the existence of watermark is known to the attackers [1]-[3]. As a comparison, steganography does not require strong robustness. Steganography transmits a secret message in a multimedia with the assumption that the existence of the message is not known. Audio watermarking algorithms were studied in [4]-[7]. In [4], audio watermarking techniques using sinusoidal patterns based on pseudo-random sequences were proposed. A watermarking algorithm by adding the watermark information in the phase spectrum in the complex Hadamard transform was examined in [5]. Digital audio watermarking techniques in real-time voice communications over IP were examined in [6]. In [7], a speech watermarking scheme that uses the sinusoidal model of speech signal for watermarking was proposed. Text watermarking algorithms were studied in [8][9]. In [8], printed document watermarking for the authentication was investigated. In [9], the character-line intersection was applied for embedding and detecting invisible watermark on a text. Watermarking algorithms for still images were studied in [10]-[14]. In [10], it was proposed that the watermarks need to be embedded in significant components of images. In [11], the discrete wavelet transform (DWT) coefficients were employed to embed watermarks in images. In [12], a new scheme for virtual machine disk images was demonstrated. In [13], new schemes were proposed for embedding data in the image based on FFT. In [14], spread spectrum approach was applied to image watermarking. The algorithm was shown to be robust to the common attacks. Video watermarking algorithms were also proposed in published research works. A reversible watermarking algorithm was developed in [15]. A blind watermarking scheme based on DWT was developed in [16]. In [18], a new algorithm was proposed for watermark embedding by combining the discrete cosine transform with the ridgelet transform. In [19], a threshold signature approach was proposed and its performance was analyzed on correctness and security. In time-domain watermarking, integer-valued watermarks are employed and watermarks can be detected by calculating the difference between the original and watermarked images. In the absence of attacks, the detected watermark is distortionless. In transform-domain, however, the watermarks are embedded in transform coefficients. After the inverse transform, the reconstructed image may not be integer-valued whether the watermark is integer-valued or not.

Without watermark masks

An embedding process is expressed as

$$x \xrightarrow{T} T(x) \xrightarrow{a\,w_0} T(x) + a\,w_0 \xrightarrow{T^{-1}} x + T^{-1}(a\,w_0) \xrightarrow{R} x + T^{-1}(a\,w_0) + e_0 \qquad (1)$$

where x is an original image and T is a linear transform. The watermark w_0 is scaled by a factor a. After embedding, the inverse transform T^{-1} and a rounding process R are employed and the round-off error is denoted as e_0. The detecting process is expressed as

$$x + T^{-1}(a\,w_0) + e_0 \xrightarrow{-x} T^{-1}(a\,w_0) + e_0 \xrightarrow{T} a\,w_0 + T(e_0)\,, \qquad (2)$$

where a watermark is detected by mapping the difference between watermarked image and the original image to transform-domain. The distortion in the detected watermark is $T(e_0)$.

To eliminate the distortion, an adjusted watermark $a\,w_0 + T(e_0)$ referred to as ***round-off watermark*** is proposed and the watermark embedding is rewritten as

$$\begin{aligned} x &\xrightarrow{T} T(x) \xrightarrow{a\,w_0 + T(e_0)} T(x) + a\,w_0 + T(e_0) \\ &\xrightarrow{T^{-1}} x + T^{-1}(a\,w_0) + e_0 \xrightarrow{R} x + T^{-1}(a\,w_0) + e_0 \end{aligned} \qquad (3)$$

From Eq.1, $x + T^{-1}(a\,w_0) + e_0$ is the output of R and hence integer-valued. Round-off errors are not generated by R in Eq.3. The detecting process in Eq. 2 remains valid. As the embedded and detected watermarks in eqns.2 and 3 are the same, the embedding-detecting is perfect.

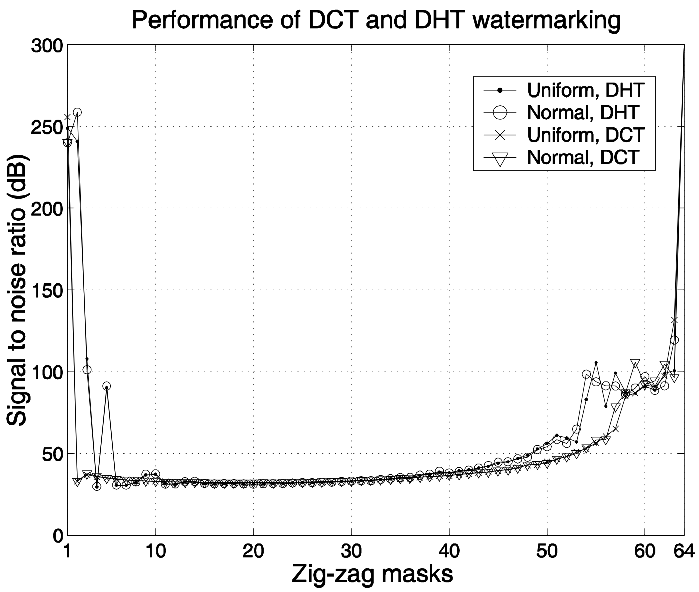

Figure 1 Watermark detection using zig-zag masks in DCT and DHT

With watermark masks

In experiments, however, it is found that the detection is not distortionless if watermark masks are employed. Fig.1 shows several watermark masks for 8×8 DCT and DHT, where only elements marked with 1 are employed in embedding and detecting. Let $F_{M\times M}$ and $a_{M\times M}$ be matrices of size $M\times M$, the element-by-element multiplication is defined, $F[a] = \left(F(m,n)\cdot a(m,n)\right)_{M\times M}$, $1 \le m,n \le M$. With masks, eqns. 1 and 2 become

$$x \overset{T}{\to} T(x) \overset{a w_0}{\to} T(x) + S[a w_0] \overset{T^{-1}}{\to} x + T^{-1}(S[a w_0]) \overset{R}{\to} x + T^{-1}(S[a w_0]) + e_1, \tag{4}$$

The watermark embedding becomes

$$x \overset{T}{\to} T(x) \overset{S[a w_0 + T(e_1)]}{\to} T(x) + S[a w_0] + S[T(e_1)] \tag{5}$$

Recall $x + T^{-1}(S[a w_0]) + e_1$ is integer-valued as it is the output of R in Eq.4. The watermarked image in Eq.5 is integer-valued if and only if the second term is integer-valued, $T^{-1}(S[T(e_1)]) - e_1 = A$, where A is a matrix with integer elements.

DC- and full-masks: Perfect detection is first shown for the full-mask $\{S(m,n) = 1,\ 1 \le m,n \le M\}$ as Eq.7 is satisfied. The DC-mask

$$S(m,n) = \begin{cases} 1, & m = n = 1, \\ 0, & otherwise. \end{cases} \tag{6}$$

is then examined. As the mean of the round-off error e_1 is 0, the DC energy of e_1 is very small. For the DCT and DHT, the upper-left element of $T(e_1)$ is the DC energy. Hence, $\tilde{S}[T(e_1)] = 0_{M \times M}$ is satisfied with very small errors or near-perfect detection is achieved.

Experimental results

Random processes with uniform distribution between $[-0.5, 0.5]$, or normal distribution with mean 0 and variance 1 are employed as watermarks. Zig-zag masks are employed. Fig.1 shows that nearly-perfect and perfect detection is achieved by the DC- and full-masks of the DCT and DHT with signal-to-noise ratio over 230 dB and 300 dB, respectively. Experiments of JPEG compression has also been conducted for several images, e.g., Lenna, Peppers, Baboon ($512 \times 512 \times 8$), and it is shown that full-band mask has good watermark performance for quality factor Q of 90 - 100. Masks using the approximation image at level-1 has the highest robustness for Q of 10 to 90. The mask using the approximation image at level-2 has the highest robustness for Q of 0 - 10. As a comparison, time-domain watermarking is perfect, but not robust for quality factor of 0 to 40.

Acknowledgements

This work was supported in part by Natural Science Foundation of China (No. 60275011), Guangdong Science Foundation (No. 021252).

References

[1] S. Bayrama, I. Avcibasa, B. Sankurb, and N. Memonc, “Image manipulation detection with binary similarity measures”, EUSIPCO - European Signal Processing Conference, September 2005.

[2] J. P. Boyer, P. Duhamel, and J. Blanc-Talon, “Game-theoretic analysis of a semi-fragile watermarking scheme based on SCS”, In Proceedings of the International Conference on Image Processing, vol. 2, pp. 1122–1125, Sep. 2005.

[3] I. Avcibas, M. Kharrazi, N. Memon, and B. Sankur,”Image steganalysis with binary similarity measures,” EURASIP J. Appl. Signal Process., vol. 17, pp. 2749–2757, 2005.

[4] Z. Liu and A. Inoue, “Audio watermarking techniques using sinusoidal patterns based on pseudorandom sequences”, IEEE Trans. Circuits Syst. Video Technol. vol. 13, no. 8, pp. 801–812, 2003.

[5] B.J. Falkowski, “Multi-polarity complex hadamard transforms for phase watermarking algorithm”, In Proceedings of the 6th Int. Conf. Information, Communication & Signal Processing, pp.1–5, 2007.

[6] F.C. Er and E. Gul, "Comparison of digital audio watermarking techniques for the security of VOIP communications", In Proceedings of the 7th Int. Conf. Information Assurance and Security (IAS) , pp. 13 – 18, 2011.
[7] M. M. Narimannejad and S. M. Ahadi, "Watermarking of speech signal through phase quantization of sinusoidal", In Proceedings of the 19th International Conference on Electrical Engineering(ICEE), pp. 1–4, 2011.
[8] C. Hrishikesh and S. Shefali, "Printed document watermarking using phase modulation", In Proceedings of the Second International Conference on Emerging Trends in Engineering and Technology(ICETET) , pp. 222–227, 2009.
[9] W. Yawai and N. Hiransakolwong, "Increase the hiding-bit capacity and strength for text watermarking with the line intersection on text image", In Proceedings of the 8th International Conference on Computing Technology and Information Management (ICCM), pp. 427 – 433, 2012.
[10] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.
[11] J. Kim, S. Hong, and S. Won, "Digital Watermarking for Cadastral Maps Using DWT", International Journal of Advancements in Computing Technology, vol. 4, no. 23, pp. 116-128, 2012.
[12] Y. Su, X. Liao, H. Jin and T. Bell, "Data hiding in virtual machine disk images", Proc. IEEE 10th Int. Conf. Computer and Information Technology (CIT), pp. 2278 – 2283, 2010.
[13] S. Riaz, M.Y. Javed and M.A. Anjum, "Invisible watermarking schemes in spatial and frequency domains", In Proceedings of the 4th Int. Conf. Emerging Technologies (ICET) , pp. 211 – 216, 2008.
[14] C. Wang, Z. Wang, and F. Chen, "Copyright Protection of Industry Design Map Based on Digital Fingerprinting", International Journal of Advancements in Computing Technology, vol. 3, no. 11, pp. 340- 345, 2011.
[15] S.-Y. Shin, H.-M. Yoo, Y.-H. Ko, H.-S. Kang and J.-W. Suh, "Reversible watermarking without underflow and overflow problems", In Proceedings of the IEEE 55th International Midwest Symp. Circuits and Systems (MWSCAS), pp. 980 – 983, 2012.
[16] C. Wang, X. Nie, X. Wan, W. Wan, and F. Chao, "A blind video watermarking scheme based on DWT, " In Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) , pp. 434--437, 2009.
[17] Y.-H. Chiou and J.-D. Lee, "Reversible Data Hiding Based on Search-order Coding VQ-compressed Images", Journal of Convergence Information Technology, vol. 6, no. 12, pp. 176-184, 2011.
[18] L. Ma, S. Wang, and Y. Zhang, "Image Feature Extraction and Watermark Technology Based on Copyright Protection", Journal of Convergence Information Technology, vol. 7, no. 23, pp. 717-725, 2012.
[19] J. Wang and Y.-Q. Cai, "Threshold Signature Scheme with Traceability and Resisting Conspiracy Attack", International Journal of Advancements in Computing Technology, vol. 4, no. 23, pp. 79-87, 2015.
[22] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 2016.
[23] N. S. Jayant and P. Noll, Digital coding of waveforms–principles and applications to speech and video. Englewood Cliffs, NJ: Prentice-Hall, 1984.
[24] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting step," J. Fourier Anal. Appl., vol. 4, no. 3, pp. 247–269, 1998.